State of Montana Information Security Advisory Council

Council Meeting Minutes
March 17, 2016
1:00 p.m.
DEQ Lee Metcalf Building – Room 111

Members Present:
Ron Baldwin, SITSD
Joe Chapman, DOJ
John Daugherty, COR
Joe Frohlich, SITSD
Stuart Fuller, DPHHS
Kreh Germaine, DNRC
Jim Gietzen, OPI
Adrian Irish, U of M
Margaret Kauska, DOR
Lynne Pizzini, SITSD
Maj. Gen. Matthew Quinn, DMA
Erika Billiet, Kalispell

Staff Present:
Jennifer Schofield
Tim Wunderwald
Noah Horan

Guests Present:
Bryan Fox, Curt Norman, Christi Mock, Suzi Krugman, Audrey Hinman, Carroll Benjamin, Tom Mandeville, Jerry Marks, Edward Sivils, Rebecca Cooper, Craig Stewart, Lance Wetzel, Sean Rivera, Michael Barbere, John Cross, Tim Kosena, Dawn Temple

Real-time Communication:
Kyle Belcher, Dan Chelini, Phillip English, Brad Flath, Chris Gleason, Mandi Hinman, Michael Jares, Jerry Kozak, Chris Kuntz, Terry Meagher, Luann Metro, Matt Pugh, Angie Riley, Irv Vavruska, James Zito, Lorin Peterson

Welcome and Introductions
Ron Baldwin welcomed the council to the March 17, 2016 MT-ISAC meeting. All members and guests were introduced.

Minutes
The council reviewed and approved the February 18, 2016 Minutes.

Business
University Incidents
Adrian Irish provided an overview of two recent information security incidents. First, the University of Montana experienced phishing attempts during January and February of 2016. The perpetrators were attempting a wire transfer scam by imitating important members of the university system. Secondly, on December 24, 2015, the University of Connecticut's (UConn) domain was hijacked. Adrian mentioned that he is concerned that a similar vulnerability exists with the .gov top-level domain.

Q: Adrian asked who controls the .gov domain.
A: Lynne Pizzini: The Federal General Services Administration controls the .gov top-level environment.

Adrian suggested that SITSD review the .gov process. The attackers exploited a weakness in the .edu domain password reset system. Adrian noted that in situations like this, two-factor authentication would be beneficial.

Enterprise Solutions
Joe Frohlich discussed antivirus enterprise solutions for servers. In October 2016, our agreement with ESET ends. The Tools Workgroup will be considering renewal. In May 2017, the Microsoft enterprise agreement will also need to be renewed. Joe said that there needs to be discussion about endpoint protection for desktops. Anyone interested in joining the Tools Workgroup should contact Joe (jfrohlich@mt.gov) or Dawn Temple (datemple@mt.gov).

Margaret Kauska discussed the state's use of OneDrive, and asked for clarification regarding its security. She mentioned that several Department of Revenue employees were using Dropbox, which is not secure or approved. MT-Drive and OneDrive for Business are secured Enterprise solutions.

Audrey Hinman explained that her staff operates the file transfer service, which includes MT-Drive. She explained the differences between MT-Drive and OneDrive for Business. OneDrive is for document storage internal to the state only. MT-Drive is used for sharing files with users outside of the state's network. MT-Drive is a function within the file transfer service, and is secured by active directory for state employees. For public access, MT-Drive is secured by ePass Montana. Transferring a file requires a state employee to either be sending or receiving. During transit, files are secured with SSL and use AES 256-bit encryption. When data is at rest on the server, files are secured with AES 256-bit encryption. State employees can establish an MT-Drive folder, and can then control permissions for public access. For non-state employees, the system is secured by two-step verification: the user must have an established ePass account; and the request is verified via email. Files received via MT-Drive undergo a full virus scan. SITSD maintains full audit records for file permissions and all upload and download events. If a state employee leaves, the MT-Drive folder becomes accessible by their supervisor.

Q: Margaret: In regards to the audit records, would you be able to track by agency?
A: Audrey: Yes.

Jerry Marks: My staff is responsible for Office 365, which includes OneDrive for Business. OneDrive for Business is stored in the Microsoft cloud, and is a function of the Sync tool within Office. Files are saved locally and then synced to the cloud. Everything is encrypted at all times. Use of OneDrive is restricted to state employees. When an employee leaves, their manager is notified and must choose what to do with the leftover data.

Q: Joe Chapman: Are you looking to allow access to OneDrive for Business from outside the state's network?
A: Jerry: Yes, but as a prerequisite, data loss protection (DLP) and rights management will be required. Microsoft is currently working on implementing DLP, and has given a tentative timeline of around six months.
Q: Joe Frohlich: Can you use OneDrive for Business from home to access your OneDrive files?
A: Jerry: Microsoft provides a web portal, and you can log in with your state active directory credentials. This allows access to web-based Office apps and your OneDrive files. They can be edited and saved back into OneDrive without leaving a copy on your home computer. This can also help prevent against saving files to USB hard drives and brining those documents with you outside the office. There is also a mobile app where you can access you OneDrive files from your smartphone.

Workgroup Follow-Up

Governor's Dashboard: Lynne discussed the Governor's Dashboard, which was approved during the last meeting as presented by the Assessment Workgroup. Beginning in April it will be provided to the Governor's Office on a monthly basis, and will also be posted to MT-ISAC's SharePoint site.

Hardening of Devices: Joe discussed the Device Hardening document, which was approved by MT-ISAC in February. A few minor changes were made to the document, based on recommendations from MT-ISAC's last meeting.

Q: Kreh Germaine: Regarding antivirus, are you envisioning an MDM solution for mobile devices?
A: Lynne: This requirement is regarding devices that communicate using the 802.11 standard. Mobile devices are not included in this category.

Workgroup Updates

Assessment Workgroup Update

Lynne Pizzini: The Workgroup has developed an assessment document that all agency security officers can use to track their agency's compliance with new security policies. The document is posted on the MT-ISAC website.

Comment: Joe Frohlich: The QuickWins column could include best practices, top twenty controls, or other new implementations. The document will be continuously improved upon.
Q: Stuart Fuller: Will the information presented in this document by the security officer be secure?
A: Lynne: This document is to be utilized by the agency, and shared to the CIO. It will not be public.

Lynne: National Cyber Security Review (NCSR): The Assessment Workgroup proposed this review document be utilized in order to give a quick overview, which will be reported to the Governor. This document will allow agencies to compare their security with corresponding agencies from other states, and is meant to be a quick overview.

Joe Frohlich: The first NCSR document for agencies to complete will be this fall. It should take about an hour and a half to complete if you know your environment well.

Q: Maj. Gen. Matthew Quinn: Was an NCSR released last fall? Did we post the question set?

A: Lynne: Yes, it was released last fall, and the question set will be added to the MT-ISAC website for everyone to review after this meeting.

MOTION: Lynne Pizzini motioned that MT-ISAC accept NCSR as its reporting mechanism from an overall perspective. Stuart Fuller seconded. The voice vote was unanimous.

Best Practices Workgroup Update

Lynne Pizzini: The Workgroup has produced a Small Incident Handling best practices document (which is available on the MT-ISAC website). This document includes step-by-step instructions to ensure uniformity across agencies.

Action Item: The Council was instructed to review the Small Incident Handling best practices document and send comments to Lynne Pizzini (lpizzini@mt.gov). The item will be placed on the next agenda for approval.

Situational Awareness Workgroup Update

Joe Frohlich: The Workgroup produced an Incident Report form, which the council had the last month to review. The only comment on this form was to remove "Cyber" from the title and add "Information" in its place to be consistent with all MT-ISAC documentation. The title was changed to reflect this. This form will be available on the MINE page under IT Professional within the Security Section, and also will be added to the MT-ISAC website.

MOTION: Lynne motioned to accept the Incident Report form.
John Daugherty seconded. The voice vote was unanimous.

Tools Workgroup Update

Joe Frohlich: The first meeting of the Tools Workgroup is Thursday, March 24, 2016, at 1 p.m., and will be hosted on Skype. The Workgroup will discuss server antivirus and Device Hardening. Update: The first meeting was held on Tuesday, March 22, 2016 at 1 p.m.

Current Threats

Sean Rivera provided an explanation of the DROWN (Decrypting RSA using Obsolete and Weakened eNcryption) threat. DROWN exploits an HTTPS vulnerability with Secure Sockets Layer (SSL) version two, which is outdated. It allows an attacker to intercept and view a shared Transport Layer Security (TLS) certificate during a file transfer. This type of attack could also compromise other TLS servers that communicate with servers that still use the older SSL version.

Sean also discussed W-2 phishing scams, which several large companies admitted they had fallen prey to in February. This type of incident is called a Business Email Compromise (BEC) attack. Sean stressed that spear-phishing attacks are best averted through education, and that empowering employees to question requests is crucial to protecting sensitive information. Sean recommended that two-party verification of sensitive data requests be considered for implementation as a standard policy.

Adjournment

Next Meeting

Thursday, April 21, 2016, State Capitol, Room 350

Open Forum

None.

Public Comment

None.

Adjourn

The meeting adjourned at 2:00 p.m.

Adopted April 21, 2016.